PROACTIVE IT / IS MONITORING FOR BUSINESS CONTINUITY PLANNING

Stanislava Šimonová, Ondřej Šprync

Introduction

An organization fulfils its business objectives which initiate priorities for the current business processes as well as for their support processes which include gaining and processing information (data). Business informatics plays a significant part in ensuring comprehensive management of enterprise (including finance, production, logistics, human resource management, etc.) and also in promoting market relations (specific applications, electronic communication, continuous evaluation of situation on the market etc.) [4], [7]. Therefore, information systems are fully intended to support business processes. In order to gain this functionality, two aspects are monitored; content and security of information system (hereinafter IS). The content of an IS must be analysed and designed in accordance with business processes which the particular IS supports. In order to do so it is required to strictly perform data analysis and follow data modelling procedures [22]. The other aspect involves security requirements (safe running or threat resistance of the IS) [23]. Business informatics represents a complicated complex which is managed within recommended methods and frameworks such as COBIT and ITIL [2], [3], [5].

Information environment (eventually its parts) is often outsourced. Outsourcing means that a company transfers responsibility for a specific information technology function to an external vendor, in other words, the practice of delegating responsibility for some to all of an organization's IS applications and operations to an outside firm [9], [12]. When outsourcing is used, some enterprise activities are ensured by external services (and resources) of a provider who specializes in integrated blocks of provided service [17]. The scope of outsourcing of business informatics is different. We can include planning and IT (Information Technology) strategies, consulting, maintenance and support, development of SW (software) for internal use of a company, IS and application running, operating business IS (e.g. SAP), terminal stations running, web services, web hosting, help desk, hotline, call centres, training and IT education. The transition to outsourcing requires an audit of the current status, mapping information needs, developing a plan of the project and defining SLA (Service Level Agreement) for individual areas and purposes, setting up of concrete metrics and respective threshold values. Typical benefits of IT services outsourcing include defined system response (defined system performance) and knowledge of the latest technologies. Outsourcing also guarantees fulfilment of predefined conditions within the SLA, substitutability of operators and administrators, especially solutions of emergency situations and reducing risk of failures of the IS. Even though information systems are the main element of supporting tools within the main business processes, a failure of an IS usually means even a suspension of proper running process instance. Therefore, availability or unavailability of IS has key influence on business continuity.

1. IT Service continuity

Business Continuity or, in other words, Business Continuity Planning is not just a goal of an organization. It is also a tool which is focused on stable availability/performance of business processes [14]. An integrated part of this approach is Disaster Recovery Planning, i.e. planning of recovery after a break down. Causes of break downs can be either large outages (terrorist events, natural disasters) or small outages (e.g.: illness or retirement of key managers, logistics problems, failure of an internal network) [6], [20]. The role of management is to create an environment that facilitates identification and tight control of the negative risks, while nurturing an environment that allows for the identification and conversion of opportunities, and their challenge to determine how much uncertainty is the organization prepared to accept [8]. a significant aspect is to ensure conditions for IT service continuity.

1.1 Ensuring the availability of an IS

IT services must be prepared, customized and robust, in order to be able to react quickly against possible failures, either by minimizing effects followed by rapid recovering of IT services, or, in better case, by preventing problem occurrence based on following monitored indicators. Unfortunately, availability is a long-term critical factor of IS. If any IS is out of order, business processes cannot be further performed until the IS recovers.

Financial consequences of IS failures consist of following coefficients – direct costs, additional work hours, lost work hours and loss of revenue (see above on Figure 1: Financial consequences of IS failures). Direct costs are closely connected with reparation of IT failures (equipment repairs, expenses for external specialists, financial sanctions for not fulfilling of contract obligations). Additional working hours represent overhead expenses linked with certain incidents (time spent on failure correction). On the other hand, lost working hours are indirect indicator of reducing revenues, for instance, non-manufactured products. Also loss of customers due to loss of reputation of an organization (customers rather go to competitors whose systems are still functional) results into loss of profits.

Fig. 1: Financial consequences of IS failures

	Known	Estimated
Revenue	Lost Revenue	Lost work hours
Cost	Direct Cost	Additional work hours

Source: [19], own adaptation

Availability of IT services is defined by terms RAS [13] – reliability (R) availability (A) and serviceability (S).

Reliability helps to, at once, detect faults and avoid them. Although detection is a significant part of the process, it is mostly omitted. The worst behaviour of a system is when operations continue running even with a fault.

Availability is measurement how often/ how long is the service/component available for usage. Measuring of availability can be expressed by following relations [14]:

Availability = operating time / (operating time + + downtime) (1)

Planned (expected) availability = MTBF / (MTBF+ + MTTR) (2)

Basic measure of availability is the ratio of operating time to total elapsed time (1). In the case the Mean Time Between Failures (MTBF) and Mean Time To Repair (MTTR) are known, the availability might be expressed on the link (2). It is obvious the availability is mostly influenced by MTTR; that means, reducing MTTR by one tenth has the same effect as tenfold increase of MTBF.

Serviceability represents the ability of the system to be repairable and reclaimable. It also helps to identify possible failures. The purpose is to detect failures without stopping the whole operations. The options to diagnose the system include regeneration programmes and diagnostic tools including monitoring.

1.2 Proactive monitoring

One of the fundamental elements of business continuity planning is proactive monitoring, or in other words, intelligent monitoring. In order to avoid unexpected failures or to resolve the problems in time before harming the operations, there is business continuity planning which increases serviceability of systems [10]. It can also be characterized as an administrator who does not wait for a user's call reporting failures, but finds out system malfunction in time or identifies signals of possible threats. Proactive monitoring detects and responds to problems of IS before the end users notify that there have been actually some problems.

Especially, this is used in such IS which have a significant portion of profit (e-shops, etc.) In these cases, such a system is required. Most of administrators of IS understand the need for application and system monitoring to increase the availability of IS. ICT (Information and Communication Technology) department staff monitors standard sources of application servers,

such as CPU (Central Processing Unit), memory usage, etc. Nevertheless, there is a wide range of additional sources for monitoring. Therefore, it is important to understand its parameters and determine which ones are more effective for failure detection and escalation. The possibilities for failure detection are following [11], [16]:

- The first option determines the situation when the administrator of a system will run all the applications at the same time, will work with them and in the case a problem occurs, he/ she will solve them by himself. However, this option is completely unrealistic for huge amount of different applications and IT systems of an organization.
- Second option is to use software tools which monitor given sources and automatically analyze when IS exceeds set-up limits. With a usage of those tools administrator can monitor their statuses, set-up limits whereby he/ she will be informed about in order to prevent the interruptions of ICT services.

2. Monitoring preparation (with usage of SW tool OpenEdge Management)

The initial situation is shown on the company where there is no proactive monitoring implemented yet. When IT services fail, the end user informs the administrator about the situation by himself. At the same time, the user may be an external user (the user comes from a different company as IT services are outsourced) or internal (the user coming from the same company as the administrator). Absence of monitoring can cause delays while failures could be already solved or restored. Consequently, it results into a situation when clients/ customers have to wait because the service is not available yet [21].

On the other hand, there is a company which has monitoring SW tools OpenEdge Management (OEM). It deals with system tools necessary for application management based on database environment called Progress. OEM allows to constant monitoring of technological infrastructure as well as showing and analyzing gained information describing statuses and trends (status history) of a given system [18]. However, the current status of the company is provided in such a wide and complex way that does not allow a quick identification of a problem.

It is necessary to create such a list of monitors which would cover sources needed for performing operations of the IS and its components. This service is provided through an outsourcing contract which determines the obligation of the supplier to monitor and, additionally, solve ICT failures. The aim of the administrator is to obtain a quick overview of information for effective solutions of critical situation of IS.

Monitoring purposes are as follows:

- Classification of controlled sources selected according to given criteria;
- Identification/ customer classification and evaluation of its influences for monitor creation;
- Creation of process modeling for creation of monitors according to customer requirements;
- Proposals of monitors controlling sources;
- Monitor settings according to categories.

2.1 Classification of controlled sources and evaluation of customer's influences for monitor creation

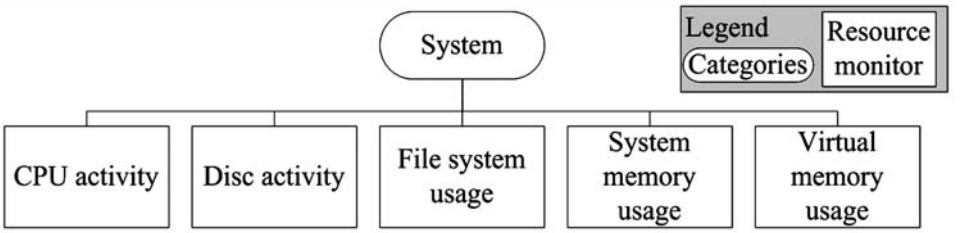
First of all, it is important to create specific technological categories into which individual monitors will be divided. Simultaneously, it is required to set up relevancy levels of problems which would classify monitors according to consequences on IS.

Sources of monitors OEM can be divided into following categories – databases, files, networks, OpenEdge environment and system sources. Furthermore, it is also demanded to set up an overview of monitors for each category (see Figure 2).

Division of monitors differs according to relevancy levels of problems. This division takes into account what the impacts on the IS are in the case of monitor source failure. However, according to OEM we can determine following levels [1], [15]:

- First severity level – Information: have just an information form with no influence on availability of IS. It constitutes mainly of notifications about successful ending up of a certain process or planning process. Notification form is provided via E-mail.
- Second severity level – Warning: warning about exceeding certain defined settings of

Fig. 2: Model of monitor overview for the category System



Source: own adaptation

monitored source or source failures without an influence on basic running of the system. Notification form is provided via E-mail and SMS. Upon the occurrence of monitoring service, the administrator is obligated to avoid shut-downs or errors of monitored sources.

- Third severity level – Error: errors which can lead to system malfunction. Notification form is provided via E-mail and SMS. Monitoring service within the administrator of IS must immediately perform proper corrective actions for all ICT recovery processes with the lowest impacts on organization or business processes.
- Fourth severity level – Severe: severe error or system malfunction. Notification form is provided via E-mail and SMS. Monitoring service within the administrator of IS must immediately perform proper corrective actions for all ICT recovery processes with the lowest impacts on organization or business processes.

As already mentioned above, the user may be either external (the user comes from another company as services are outsourced) or internal (the user coming from the same company as the administrator). Therefore, it is necessary to consider whether the model procedure is suitable for both types of customers or whether there are certain customer specifications required. In the case of business modelling, such a situation can

Tab. 1: File system usage monitor

Monitor	File System Usage
Category	System
Severity level	Error
Measurable criteria	Preference of extreme value
Description	Notification is sent when the usage of volume exceeds 80% limit of total capacity.

Source: own adaptation

Tab. 2: Utilization of disk drive monitor

Monitor	Disc activity (utilization of disk drive).
Category	System.
Severity level	Warning.
Measurable criteria	Preference of extreme value and relevancy levels.
Description	Notification is sent when the utilization of disk drive of writeable and readable operations exceeds 90% limit.

Source: own adaptation

occur when requirements for monitor creation come from supplier's staff who is an internal customer at the same time; it may have following reasons such as performance monitoring or tuning of IS running. Concerning the external customer, who represents the company which ordered monitoring service of IS, they determine the requirements for monitoring sources necessary for constant running of the IS. As already remarked, there is no need to divide customers into internal or external. The reason is that both types have the same requirements for source monitoring and demand the same monitor output.

3. Model processes enabling creation of monitors according to customer requirements and design of monitors of tracked sources

The model of the process "Monitor creation according to customer requirements" (see figure 3) shows activities to be performed based on customer requirements for monitoring of certain sources. Division of customer types is not taken into account in the model because they both have the same requirements for source monitoring and demand the same monitor output.

In the next step, proposals of monitors of tracked sources are made accordingly with categories which are defined in the previous step; Monitors Proposals Examples (see figures 1 and 2).

3.1 Monitor settings according to categories

By default settings of monitors there are defined rules showing which sources will be monitored. Among others, we have to determine an interval in which the rule will be repeating and monitoring the status of a source. The amount of notifications signifies how many times we can exceed the rules before the message is generated for service department. Finally, it is necessary to set up the relevancy level of the monitor. Examples of setting up the rules are demonstrated in Table 3 and Table 4.

3.2 Verification

The created model was verified based on requirements of external or internal customer.

The external customer required web self-service monitoring. Thanks to the analysis of such a requirement it was found out that the monitor belongs to category called "network" and is feasible. Therefore, the monitor was assigned to the second relevancy level (warning) because source failure does not cause a danger for whole IS. Consequently, there have been determined rules – see Table 5 (the amount of notifications signifies how many times we can exceed the rules until the message is generated for the service department). Also, the value of error messages was analyzed and chosen a suitable type of monitor. Based on the availability analysis of source, it was

Tab. 3: Setting up the rules for category System

Monitor	Rule	Interval	Notification	Severity level
File volume /zpone/data	Usage: 90 % and more	5 mins	1	Error
Capacity utilization of floppy disk drives	Utilization: 90 % and more	5 mins	2	Warning

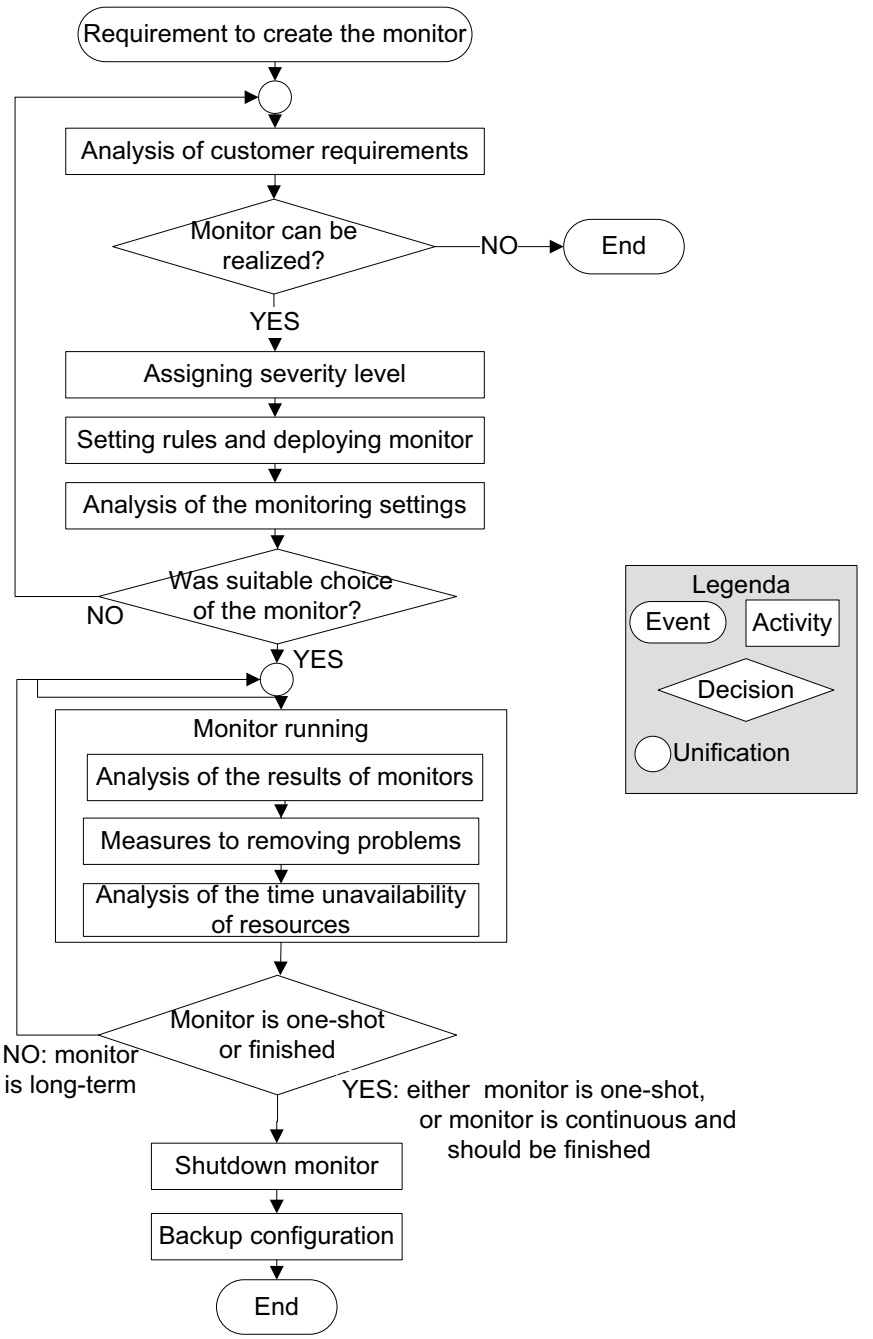
Source: own adaptation

Tab. 4: Setting up the rules for category OE - databases

Monitor	Rule	Interval	Notification	Severity level
Abnormal shutdown of database	Presence of keyword in database log	5 mins	1	Severe
Normal shutdown of database	Presence of keyword in database log	5 mins	1	Information

Source: own adaptation

Fig. 3: Model processes of setting up a monitor according to customer's requirements



Source: own

Tab. 5: Monitor's rule for external customer

Monitor	Rule	Interval	Notification	Severity level
Web self-service (TCP)	The answer exceeds 500 ms or without an answer 2000 ms	2 mins	1	Error

Source: own adaptation

identified that the value of the failure of web-self service ranged in minutes; while during non monitoring of operation it ranged in tens of minutes or hours; mostly reclaimed by customer's clients. The last step included back-up and documentation of the monitor configuration.

The internal customer (staff of developing department) required monitoring of long transactions. The reason is that information about loss of already created entries in database came from the external customer. Therefore, there has to be a proper program invented to monitor a length of transactions. Results were entered into an output log which tracks presence of the keyword.

Thanks to the analysis of requirement it was detected that the monitor belongs to the 'file' category and that is feasible. The monitor was assigned to first relevancy level (warning) due to informational notification without effects on functioning of the IS. Consequently, rules have been determined – see Table 6. Also, the value of error messages was analyzed and chosen a suitable type of monitor. Based on the results of the analysis of performance monitoring results, there have been made several arrangements which solve the performance problems of the IS. Afterwards, the monitor was turned off and a back up of configuration was made.

4. Conclusion

Existence of business continuity is important for every organization. It consists of planning failure recovery when the cause can be even failure of computer network. Even though, information systems belong to supporting tools from the view of main business processes, the IT failure usually means stopping the whole operations. Therefore, the availability or unavailability has the main influence on business continuity. IT service continuity occurs when services are prepared, customized and robust, in order to be able to quickly react against possible failures by minimizing effects followed by rapid recovering of IT services. One of the fundamental elements of business continuity planning is proactive monitoring. The element can be also characterized as an administrator who is not waiting for a user's call for failures, but finds out system malfunction in time or identifies signals of possible threats. Proactive monitoring detects and responds to problems of IS before the end users notify there have been actually some problems. My work is focused on usage of SW tools which monitor chosen sources and automatically inform while defined limits exceed. The administrator can monitor their status, setting up the limits which prevent ICT failures. Monitor creation procedures are following - classification of monitored sources according to criteria, identification/classification of customer and evaluating its influence for monitor creation based on customer requirements, proposal of monitor controlled sources, and settings of monitors divided by categories. The created model was verified on SW tools OpenEdge.

References:

[1] BACKMAN, A. *OpenEdge Revealed: Mastering the OpenEdge Database with OpenEdge Management.* Release 3.1C. Bedford (Massachusetts): Progress Software Corporation, 2008. 266 p. ISBN 978-0-923562-08-3.

[2] CARTLIDGE, A. a kol. *Úvodní přehled ITIL.V3.* Praha: Hewlett-Packard s.r.o., 2007. 56 s. ISBN 0-95551245-8-1.

Tab. 6: Monitor's rule for external customer

Monitor	Rule	Interval	Notification	Severity level
Control of long transactions	Presence of keyword in transaction log	5 mins	1	Control of long transactions

Source: own adaptation

[3] COBIT. *Control Objectives for Information and Related Technology,* 4.1. [online]. [cit. 2010-06-21]. Available on: <http://www.isaca.org/Knowledge--Center/cobit/Pages/ Downloads.aspx>.
[4] DOUCEK, P. Řízení bezpečnosti informačních systémů. *E+M Ekonomie a Management.* 2006, Vol. 9, Iss. 2, pp. 123-141. ISSN 1212-3609.
[5] DOUCEK, P., NOVOTNÝ, O. Standardy řízení podnikové informatiky. *E+M Ekonomie a Management.* 2007, Vol. 10, Iss. 3, pp. 132-146. ISSN 1212-3609.
[6] FULMER, K. L., *Business Continuity Planning.* Brookfield: Rothstein Associates, 2005. 180 p. ISBN 1-931332-21-5.
[7] GÁLA, L., POUR, J., TOMAN, P. *Podniková informatika.* 1st ed. Praha: Grada, 2006. 484 s. ISBN 80-247-1278-4.
[8] GRAHAM, J. and KAYE, D. *A Risk Management Approach to Business Continuity: Aligning Business Continuity with Corporate Governance.* USA: Rothstein Associates Inc., 2006. 401 s. ISBN 1-931332-36-3.
[9] HOFFER, J., GEORGIE, J., VALACICH, J. *Modern Systems Analysis and Design.* New Jersey: Prentice Hall, 2004. 683 s. ISBN 0-13-145461-7.
[10] IT MANAGEMENT. *Proaktivní monitoring* [online]. [cit. 2010-06-24]. Available on: <http://www.itmanagement.cz/view.php?nazevclanku=proaktivni-monitoring&cisloclanku=2009060002>.
[11] KAČMAŘÍK, R. *Citrix EdgeSight: proaktivní monitoring IT prostředí* [online]. 2007, roč. 2, č. 1 [cit. 2010-06-23]. 59 p. (PDF). Available on: <http:// www. arrowecs.cz /web/infobaze.nsf/ info/readme_1_2007/ $file/Citrix%20EdgeSight.pdf>.
[12] MALAGA, R. *Information Systems Technology.* New Jersey: Prentice Hall, 2005. 386 p. ISBN 0-13-049750-9.
[13] MITCHELL, J., HENDERSON, J. A. and VILLARREAL, J. IBM *Power Platform Reliability, Availability, and Serviceability (RAS)* [online]. [cit. 2010-06-24]. Available on: <ftp://public.dhe.ibm.com/common /ssi/sa/wh/n/pow03003usen/ POW03003USEN.PDF>.
[14] OKOLITA, K. *Building an Enterprise-Wide Business Continuity Program.* CRC Press, 2009. 344 p. ISBN 978-1420088649.
[15] OpenEdge® Management: *Alerts Guide and Reference* [online]. Release 10.2 A. Bedford (Massachusetts): Progress Software Corporation, 2009 [cit. 2010-06-22]. Available on: <http://communities.progress.com/pcom/servlet/JiveServlet/download/16371-1-15495/far.pdf>.
[16] POLOZOFF, A. IBM: *Technical library* [online]. [cit. 2010-06-25]. Proactive Application Monitoring. Available on: <http://www.ibm.com/ developerworks/websphere/library/techarticles/ 0304_polozoff/ polozoff.html>.
[17] RYDVALOVÁ, P. a RYDVAL, J. *Outsourcing ve firmě.* Brno: Computer Press, 2007. 102 p. ISBN 978-80-251-1807-8.
[18] SABO, J. Dostupnost především. *Progress: Magazín profesionálních uživatelů Progressu* [online]. 2004, Vol. 10, Iss. 1, [cit. 2010-06-25]. 24 p. (PDF). Available on: <http://www.progress.com/progress_software/worldwide_sites/cz/docs/casposis/070913d.pdf>.
[19] SCHMIDT, K. *High Availability and Disaster Recovery:* Concepts, Design, Implementation. 1st ed. Berlin: Springer, 2006. 410 p. ISBN 978-3-540-24460-8.
[20] SLATER, D. *Business Continuity and Disaster Recovery Planning: The Basics* [online]. [cit. 2010-06-22]. Available on: <http://www.csoonline.com/article/204450/ business-continuity-and-disaster--recovery-planning-the-basics>.
[21] ŠPRYNC, O. *Efektivní monitoring databáze pro zvýšení výkonnosti IS.* Univerzita Pardubice: bakalářská práce, 2010. 59 s.
[22] VRANA, I. a RICHTA, K. *Zásady a postupy zavádění podnikových informačních systémů.* 1st ed. Praha: Grada, 2005. 188 s. ISBN 80-247-1103-6.
[23] WIEGERS, K. *Požadavky na software.* 1st ed. Brno: Computer Press, a.s., 2008. 448 s. ISBN 978-80-251-1877-1.

Ing. Stanislava Šimonová, Ph.D.
University of Pardubice
Faculty of Economics and Administration
Institute of System Engineering and Informatics
Stanislava.Simonova@upce.cz

Ondřej Šprync
Database administrator
Pike Electronic s.r.o.
Jeseniova 1196/52, 130 00 Praha 3
OSprync@pikeelectronic.com

Doručeno redakci: 19. 10. 2010
Recenzováno: 11. 11. 2010, 21. 3. 2011
Schváleno k publikování: 1. 7. 2011

ABSTRACT

PROACTIVE IT / IS MONITORING FOR BUSINESS CONTINUITY PLANNING

Stanislava Šimonová, Ondřej Šprync

An organization fulfils its business objectives which initiate priorities for the current business processes as well as for their means of support which include gaining and processing information (data). Information systems are a significant means of support which are used by company in order to meet business objectives. Information systems are fully intended to support business processes. In order to gain this functionality, there are two aspects monitored, which are content and safety of the information system. Failure or shut-down of information system has an important influence on business processes realization or, in other words, has influence on business continuity. Existence of business continuity is important for every organization. It consists of planning failure recovery when the cause can be even the failure of computer network. Even though information system belongs to supporting tools from the view of main business processes, IT failure usually means stopping the whole operations. Therefore, the availability or unavailability has the main influence on business continuity. IT service continuity occurs when services are prepared, customized and robust, in order to be able to quickly react against possible failures by minimizing effects followed by rapid recovering of IT services.

Therefore, it is required to identify threats of information system failures before it is too late. In order to detect abnormal statuses of information systems it is needed to perform appropriate measures in time. One of the possibilities to avoid failures of IT services in time is proactive monitoring. The text deals with the process of creating and verification of a model enabling creation of monitors according to customer requirements.

Key words: *business continuity, information system, proactive monitoring.*

JEL Classification: *L86, M11, M15.*